Noncatastrophic convolutional codes over a finite ring

D. Napp[a], R. Pinto[b], C. Rocha[*,c]

[a]*Departament de Matemàtiques, Universitat d'Alacant, Spain.*
[b]*Department of Mathematics, University of Aveiro, Portugal.*
[c]*Instituto Superior de Contabilidade e Administração de Coimbra, Instituto Politécnico de Coimbra, Portugal.*

Abstract

Noncatastrophic encoders are an important class of polynomial generator matrices of convolutional codes. When these polynomials have coefficients in a finite field, these encoders have been characterized are being polynomial left prime matrices. In this paper we study the notion of noncatastrophicity in the context of convolutional codes when the polynomial matrices have entries in a finite ring. In particular, we need to introduce two different notion of primeness in order to fully characterize noncatastrophic encoders over the finite ring $\mathbb{Z}_{p^r}$. The second part of the paper is devoted to investigate the notion of free and column distance in this context when the convolutional code is a free finitely generated $\mathbb{Z}_{p^r}$-module. We introduce the notion of b-degree and provide new bounds on the free distances and column distance. We show that this class of convolutional codes is optimal with respect to the column distance and to the free distance if and only if its projection on $\mathbb{Z}_p$ is.

1. Introduction

The notion of primeness plays a central role in the polynomial matrix approach to several areas of pure and applied mathematics, such as systems and control theory or coding theory. In this paper we consider polynomial matrices over the finite ring $\mathbb{Z}_{p^r}$, where p is a prime and r an integer greater than 1. Our motivation for considering such a finite ring $\mathbb{Z}_{p^r}$ stems from applications in the area of error-correcting codes and in particular of convolutional codes over $\mathbb{Z}_{p^r}$. Such a ring is useful for the so-called coded modulation scheme where

*Corresponding author

[1]This work is supported by The Center for Research and Development in Mathematics and Applications (CIDMA) through the Portuguese Foundation for Science and Technology (FCT - Fundação para a Ciência e a Tecnologia), references UIDB/04106/2020 and UIDP/04106/2020. Diego Napp is partially supported by Ministerio de Ciencia e Innovación via the grant with ref. PID2019-108668GB-I00.

the codewords in $\mathbb{Z}_{p^r}$ are mapped onto phase-shift-keying (PSK) modulation signals sets. The mapping is such that distances between modulation points are preserved under additive operations in $\mathbb{Z}_{p^r}$, see [26] for more details. In [17] Massey and Mittelholzer observed for the first time that convolutional codes over $\mathbb{Z}_M$, are the most appropriate class of codes for phase modulation. Note that even though we will focus on the ring $\mathbb{Z}_{p^r}$, by the Chinese Remainder Theorem, results on codes over $\mathbb{Z}_{p^r}$ can be extended to codes over $\mathbb{Z}_M$.

An important concept in the theory of convolutional codes is the noncatastrophicity. When a catastrophic convolutional generator matrix is used for encoding, finitely many errors in the estimate of the transmitted codeword can lead to infinitely many errors in the estimate of the information sequence. This is of course a catastrophic situation that has to be avoided when designing the generator matrix. Noncatastrophic generator matrices have been characterized as left prime polynomial matrices and have been studied in several contexts depending on the definition considered in each case, see [1, 11, 21, 22]. In this work we define convolutional codes as finitely generated free $\mathbb{Z}_{p^r}[d]$-modules of $\mathbb{Z}_{p^r}[d]^n$, where $\mathbb{Z}_{p^r}[d]$ is the polynomial ring with coefficients in $\mathbb{Z}_{p^r}$ and study noncatastrophicity in this setting [13, 18, 19, 25]. In the case of matrices with entries in $\mathbb{Z}_{p^r}[d]$ we need to distinguish two types of left primeness, namely, zero left prime and factor left prime, as happens in the case of polynomial matrices in several variables over a field [15, 20, 24, 28]. We provide a characterization of zero left prime polynomial matrices from which it follows that when a convolutional code admit a left zero prime generator matrix, i.e., a noncatastrophic encoder, then the code can be described by means of a parity-check polynomial matrix.

The second part of the paper is devoted to investigating the Hamming distances of these codes as these will determine their error-correcting capabilities. In the context of convolutional codes the column distance is arguably the most important notion of distance [9] and therefore we shall focus on the study of this particular distance. To this end we introduce a novel notion, called the b-degree, and derive bounds on the column distance in terms of the dimension, length and b-degree. In [21] it was proven that the free distance of convolutional codes over $\mathbb{Z}_{p^r}$ it is determined by its projection over $\mathbb{Z}_p$. The authors used this fact and the Hensel lift of a cyclic code in [21] to build optimal convolutional codes with respect to the free distance. Here we show that a convolutional code over $\mathbb{Z}_p$ is optimal with respect to the column distance if and only if its projection is. This will allow the construction of optimal convolutional codes over $\mathbb{Z}_{p^r}$ from well-known classes of convolutional codes over $\mathbb{Z}_p$.

The results of the paper are twofold: we first analyse the primeness of polynomial matrices with entries in $\mathbb{Z}_{p^r}[d]$ in Section 2 and second we investigate the column distances of free convolutional codes over $\mathbb{Z}_{p^r}$ in Section 3. In each section we briefly provide some preliminaries: in Section 2 we recall known results of primeness of polynomial matrices over finite fields and in Section 3 the definitions of convolutional codes, free distance and column distances are

presented.

2. Primeness of polynomial matrices over $\mathbb{Z}_{p^r}$

We denote by $\mathbb{F}[d]$ the ring of polynomials in the indeterminate d and coefficients in a finite field $\mathbb{F}$ and by $\mathbb{F}(d)$ the field of rational functions defined in $\mathbb{F}$. Next we will present results that are well-known in the literature, see [5, 6] for more details.

2.1. Primeness of polynomial matrices over a finite field $\mathbb{F}$

Definition 2.1. *A polynomial matrix $U(d) \in \mathbb{F}[d]^{k\times k}$ is unimodular if it is invertible and $U(d)^{-1} \in \mathbb{F}[d]^{k\times k}$.*

Lemma 2.1. *Let $U(d) \in \mathbb{F}[d]^{k\times k}$. Then $U(d)$ is unimodular if and only if $\det U(d) \in \mathbb{F}\backslash\{0\}$.*

Definition 2.2. *A polynomial matrix $A(d) \in \mathbb{F}[d]^{k\times n}$ is left prime if in all factorizations*

$$A(d) = \Delta(d)\bar{A}(d), \text{ with } \Delta(d) \in \mathbb{F}[d]^{k\times k}, \text{ and } \bar{A}(d) \in \mathbb{F}[d]^{k\times n},$$

the left factor $\Delta(d)$ is unimodular.

Left prime matrices admit several characterizations as stated in the next theorem.

Theorem 2.1. *Let $A(d) \in \mathbb{F}[d]^{k\times n}$. The following are equivalent:*

1. *$A(d)$ is left prime;*
2. *there exist unimodular matrices $U(d) \in \mathbb{F}[d]^{k\times k}$ and $V(d) \in \mathbb{F}[d]^{n\times n}$ such that*
$$U(d)A(d)V(d) = [I_k \;\; 0];$$
3. *there exists a unimodular matrix $V(d) \in \mathbb{F}[d]^{n\times n}$ such that $A(d)V(d) = [I_k \;\; 0]$;*
4. *there exists $B(d) \in \mathbb{F}[d]^{(n-k)\times n}$ such that $\begin{bmatrix} A(d) \\ B(d) \end{bmatrix}$ is unimodular;*
5. *$A(d)$ admits a polynomial right inverse;*
6. *for all $u(d) \in \mathbb{F}(d)^k$, $u(d)A(d) \in \mathbb{F}[d]^n$ implies that $u(d) \in \mathbb{F}[d]^k$;*
7. *$A(\alpha)$ has rank k for all $\alpha \in \bar{\mathbb{F}}$, where $\bar{\mathbb{F}}$ denotes the algebraic closure of $\mathbb{F}$;*
8. *the ideal generated by all the k-th order minors of $A(d)$ is $\mathbb{F}[d]$.*

2.2. Primeness of polynomial matrices over $\mathbb{Z}_{p^r}$

In this section we study the notion of left prime for polynomial matrices over $\mathbb{Z}_{p^r}$. We denote by $\mathbb{Z}_{p^r}[d]$ the ring of polynomials in the indeterminate d, with coefficients in $\mathbb{Z}_{p^r}$ and by $\mathbb{Z}_{p^r}(d)$ the ring of rational functions defined, see [8], as the set

$$\left\{ \frac{p(d)}{q(d)} : p(d), q(d) \in \mathbb{Z}_{p^r}[d] \text{ and the coefficient of the smallest power of } d \text{ in } q(d) \text{ is a unit} \right\}.$$

This condition allows us to treat a rational function as an equivalence class in the relation

$$\frac{p(D)}{q(D)} \sim \frac{p_1(D)}{q_1(D)} \text{ if and only if } p(D)q_1(D) = p_1(D)q(D).$$

Any element $a \in \mathbb{Z}_{p^r}$ has a p-adic expansion [3], *i.e.*, it can be written uniquely as a linear combination of $1, p, p^2, \dots \ \dots, p^{r-1}$, with coefficients in $\mathcal{A}_p = \{0, 1, \dots, p-1\} \subset \mathbb{Z}_{p^r}$,

$$a = \alpha_0 + \alpha_1 p + \cdots + \alpha_{r-1} p^{r-1}, \ \ \alpha_i \in \mathcal{A}_p, \ \ i = 0, 1, \dots, r-1.$$

Note that all elements in $\mathcal{A}_p \backslash \{0\}$ are units. Given a matrix $A(d) \in \mathbb{Z}_{p^r}[d]^{k \times n}$, denote by $[A(d)]_p$ its (componentwise) projection into $\mathbb{Z}_p$.

Definition 2.3. *A polynomial matrix $U(d) \in \mathbb{Z}_{p^r}[d]^{k \times k}$ is unimodular if it is invertible and $U(d)^{-1} \in \mathbb{Z}_{p^r}[d]^{k \times k}$.*

Next lemma characterizes the polynomial matrices over $\mathbb{Z}_{p^r}[d]$ which admit a right polynomial inverse.

Lemma 2.2. *A polynomial matrix $A(d) \in \mathbb{Z}_{p^r}[d]^{k \times n}$, with $n \geq k$, admits a polynomial right inverse if and only if $[A(d)]_p \in \mathbb{Z}_p[d]^{k \times n}$ also admits a polynomial right inverse over $\mathbb{Z}_p[d]$.*

Proof 1. *If $[A(d)]_p$ admits a polynomial right inverse over $\mathbb{Z}_p[d]$ then there exists $B(d) \in \mathbb{Z}_p[d]^{n \times k}$ such that*

$$[A(d)]_p B(d) = I_k \mod p.$$

Considering $B(d)$ as a matrix over $\mathbb{Z}_{p^r}[d]$, we have that

$$A(d)B(d) = I_k - pX(d),$$

for some $X(d) \in \mathbb{Z}_{p^r}[d]^{k \times k}$ and therefore

$$B(d)(I_k + pX(d) + p^2 X^2(d) + \cdots + p^{r-1} X^{r-1}(d))$$

is a right inverse of $A(d)$. The converse is obvious.

The following theorem is immediate.

Theorem 2.2. *Let $U(d) \in \mathbb{Z}_{p^r}[d]^{k\times k}$. The following are equivalent:*

1. *$U(d)$ is unimodular;*
2. *$\det U(d)$ is a unit;*
3. *$[U(d)]_p$ is unimodular in $\mathbb{Z}_p[d]^{k\times k}$.*

Left primeness is a property of polynomial matrices which plays a fundamental role when we consider convolutional codes over a finite field $\mathbb{F}$. As mentioned before, a polynomial matrix $A(d) \in \mathbb{F}[d]^{k\times n}$ is left prime if in all factorizations

$$A(d) = \Delta(d)\tilde{A}(d), \text{ with } \Delta(d) \in \mathbb{F}[d]^{k\times k}, \text{ and } \tilde{A}(d) \in \mathbb{F}[d]^{k\times n},$$

the left factor $\Delta(d)$ is unimodular, or equivalently if the ideal generated by all the k-th order minors of $A(d)$ is $\mathbb{F}[d]$ (see Theorem 2.1). However, this equivalence does not hold over $\mathbb{Z}_{p^r}$. There are polynomial matrices over $\mathbb{Z}_{p^r}[d]$ that satisfy the former condition but do not satisfy the later, as it is illustrated in the following example.

Example 2.1. *The matrix*

$$A(d) = \begin{bmatrix} 1+3d & 1+d \end{bmatrix} \in \mathbb{Z}_4[d]^2$$

does not have a nonunimodular left factor, but the ideal generated by its full size minors is

$$\{(1+d)p(d) \,:\, p(d) \in \mathbb{Z}_{p^r}[d]\}.$$

Therefore, we need to introduce two different notions of primeness when dealing with polynomial matrices over $\mathbb{Z}_{p^r}$.

Definition 2.4. *A polynomial matrix $A(d) \in \mathbb{Z}_{p^r}[d]^{k\times n}$ is left factor-prime (ℓFP) if in all factorizations*

$$A(d) = \Delta(d)\bar{A}(d) \text{ with } \Delta(d) \in \mathbb{Z}_{p^r}[d]^{k\times k} \text{ and } \bar{A}(d) \in \mathbb{Z}_{p^r}[d]^{k\times n},$$

the left factor $\Delta(d)$ is unimodular.

Definition 2.5. *A polynomial matrix $A(d) \in \mathbb{Z}_{p^r}[d]^{k\times n}$ is left zero-prime (ℓZP) if the ideal generated by all the k-th order minors of $A(d)$ is $\mathbb{Z}_{p^r}[d]$.*

Right factor-prime (rFP) and right zero-prime (rZP) matrices are defined in the same way, upon taking transposes.

Remark 2.1. *Note that the fact that the conditions of Theorem 2.1 are not anymore equivalent when considering rings instead of fields also occurs when considering the polynomial ring $\mathbb{F}[d_1, \ldots, d_n]$ in several variables instead of $\mathbb{F}[d]$, see [15, 16, 20, 24, 28] for more details.*

As shown in Example 2.1 factor-primeness does not imply zero-primeness, however the converse is true as stated in the following lemma.

Lemma 2.3. *Let $A(d) \in \mathbb{Z}_{p^r}[d]^{k\times n}$. If $A(d)$ is left zero-prime then it is also left factor-prime.*

Proof 2. *Let us assume that $A(d)$ is not left factor prime. Then $A(d) = X(d)\tilde{A}(d)$ for some $\tilde{A}(d) \in \mathbb{Z}_{p^r}[d]^{k\times n}$ and $X(d) \in \mathbb{Z}_{p^r}[d]^{k\times k}$ nonunimodular. Then by Theorem 2.2 $x(d) = \det X(d)$ is not a unit and the ideal generated by all the k-th order minors of $A(d)$ is contained in $\{x(d)p(d) : p(d) \in \mathbb{Z}_{p^r}[d]\}$. Consequently, $A(d)$ is not left zero-prime.*

It is easy to see that an ideal $\mathcal{I}$ of $\mathbb{Z}_{p^r}[d]$ is equal to $\mathbb{Z}_{p^r}[d]$ if and only if $[\mathcal{I}]_p = \{[u]_p : u \in \mathcal{I}\}$ is equal to $\mathbb{Z}_p[d]$ and, therefore, the next lemma follows immediately.

Lemma 2.4. *$A(d) \in \mathbb{Z}_{p^r}[d]^{k\times n}$ is left zero-prime over $\mathbb{Z}_{p^r}[d]$ if and only if $[A(d)]_p \in \mathbb{Z}_p[d]^{k\times n}$ is left prime over $\mathbb{Z}_p[d]$.*

Now, we are in position to prove the following characterizations of left zero-prime matrices with entries in $\mathbb{Z}_{p^r}$ which can be considered as an extension of Theorem 2.1 to the finite ring case.

Theorem 2.3. *Let $A(d) \in \mathbb{Z}_{p^r}[d]^{k\times n}$. The following are equivalent:*

1. *$A(d)$ is left zero-prime;*
2. *there exist unimodular matrices $U(d) \in \mathbb{Z}_{p^r}[d]^{k\times k}$ and $V(d) \in \mathbb{Z}_{p^r}[d]^{n\times n}$ such that $U(d)A(d)V(d) = [I_k \;\; 0]$;*
3. *there exists a unimodular matrix $V(d) \in \mathbb{Z}_{p^r}[d]^{n\times n}$ such that $A(d)V(d) = [I_k \;\; 0]$;*
4. *there exists $B(d) \in \mathbb{Z}_{p^r}[d]^{(n-k)\times n}$ such that $\begin{bmatrix} A(d) \\ B(d) \end{bmatrix}$ is unimodular;*
5. *$A(d)$ admits a polynomial right inverse;*
6. *for all $u(d) \in \mathbb{Z}_{p^r}(d)^k$, $u(d)A(d) \in \mathbb{Z}_{p^r}[d]^n$ implies that $u(d) \in \mathbb{Z}_{p^r}[d]^k$;*
7. *$\bar{A}(\alpha)$ has rank k, $\bmod p$, for all $\alpha \in \bar{\mathbb{Z}}_p$, where $\bar{\mathbb{Z}}_p$ denotes the algebraic closure of $\mathbb{Z}_p$ and $\bar{A}(d) = [A(d)]_p$.*

Proof 3. *From Theorems 2.1 and 2.2 and Lemma 2.4 we immediately conclude that 2) $\Rightarrow$ 1), 3) $\Rightarrow$ 1), 4) $\Rightarrow$ 1), 5) $\Rightarrow$ 1), 7) $\Rightarrow$ 1) and 1) $\Rightarrow$ 7). Next we prove the implications 1) $\Rightarrow$ 2), 2) $\Rightarrow$ 3), 3) $\Rightarrow$ 4), 4) $\Rightarrow$ 5), 5) $\Rightarrow$ 6) and 6) $\Rightarrow$ 1).*

1) $\Rightarrow$ 2): Since $A(d)$ is ℓZP, $[A(d)]_p$ is left prime over $\mathbb{Z}_p[d]$ and therefore there exist unimodular matrices $U(d) \in \mathbb{Z}_p[d]^{k\times k}$ and $V(d) \in \mathbb{Z}_p[d]^{n\times n}$ such that

$$U(d)[A(d)]_pV(d) = [I_k \;\; 0] \mod p.$$

Considering $U(d)$ and $V(d)$ as matrices over $\mathbb{Z}_{p^r}[d]$ we have that

$$U(d)A(d)V(d) = [X_1(d) \;\; X_2(d)],$$

with $X_1(d) \in \mathbb{Z}_{p^r}[d]^{k\times k}$ *and* $X_2(d) \in \mathbb{Z}_{p^r}[d]^{k\times(n-k)}$*. Note that,* $X_1(d)$ *is unimodular because* $[X_1(d)]_p = I_k$ *and that* $U_1(d) = X_1(d)^{-1}U(d)$ *and*

$$V_1(d) = V(d)\begin{bmatrix} I_k & -X_1(d)^{-1}X_2(d) \\ 0 & I_{n-k} \end{bmatrix}$$

are polynomial matrices. It is easy too see that $U_1(d)$ *and* $V(d)$ *are unimodular matrices, and that*

$$U_1(d)A(d)V_1(d) = [I_k \ \ 0].$$

2) $\Rightarrow$ 3)*: Let* $U(d) \in \mathbb{Z}_{p^r}[d]^{k\times k}$ *and* $V(d) \in \mathbb{Z}_{p^r}[d]^{n\times n}$ *be unimodular matrices such that* $U(d)A(d)V(d) = [I_k \ \ 0]$*. Then* $A(d)V(d) = [U(d)^{-1} \ \ 0]$ *and, therefore*

$$V_1(d) = V(d)\begin{bmatrix} U(d) & 0 \\ 0 & I_{n-k} \end{bmatrix}$$

is a unimodular matrix such that $A(d)V_1(d) = [I_k \ \ 0]$*.*

3) $\Rightarrow$ 4)*: From the assumption* $A(d) = [I_k \ 0]\tilde{V}(d)$ *for some unimodular matrix* $\tilde{V}(d) \in \mathbb{Z}_{p^r}[d]^{n\times n}$*, i.e.,* $A(d)$ *is the submatrix of* $\tilde{V}(d)$ *constituted by its first* k *rows.*

4) $\Rightarrow$ 5)*: Let* $[X(d) \ \ Y(d)]$ *with* $X(d) \in \mathbb{Z}_{p^r}[d]^{n\times k}$ *and* $Y(d) \in \mathbb{Z}_{p^r}[d]^{n\times(n-k)}$ *be such that*

$$\begin{bmatrix} A(d) \\ B(d) \end{bmatrix}\begin{bmatrix} X(d) & Y(d) \end{bmatrix} = I_n.$$

Then $A(d)X(d) = I_k$*.*

5) $\Rightarrow$ 6)*: Let* $u(d) \in \mathbb{Z}_{p^r}(d)^k$ *be such that* $u(d)A(d) = w(d) \in \mathbb{Z}_{p^r}[d]^n$ *and let* $X(d) \in \mathbb{Z}_{p^r}[d]^{n\times k}$ *be a right inverse of* $A(d)$*. Then* $u(d) = w(d)X(d)$*, which is a polynomial vector.*

6) $\Rightarrow$ 1)*: Let us assume that* $A(d)$ *is not* ℓZP*. Then* $[A(d)]_p$ *is not left prime over* $\mathbb{Z}_p[d]$*, and therefore there exists a nonpolynomial vector* $u(d) \in \mathbb{Z}_p(d)^k$ *such that* $u(d)[A(d)]_p \in \mathbb{Z}_p[d]^n \mod p$*. Considering* $u(d)$ *as a vector over* $\mathbb{Z}_{p^r}[d]$*, it follows that* $p^{r-1}u(d) \in \mathbb{Z}_{p^r}[d]^k$ *is also nonpolynomial and* $p^{r-1}u(d)A(d) \in \mathbb{Z}_{p^r}[d]^n$*.*

3. Distance properties of free convolutional codes over $\mathbb{Z}_{p^r}$

In this section we first recall the basic definitions of convolutional codes over $\mathbb{Z}_{p^r}$. We consider convolutional codes as free $\mathbb{Z}_{p^r}[d]$-submodules of $\mathbb{Z}_{p^r}[d]^n$, for some $n \in \mathbb{N}$, see [13, 18, 19, 25]. We require the encoding map to be injective and therefore focus on free submodules of $\mathbb{Z}_{p^r}[d]^n$. We note that different definitions have been considered in the literature, see for instance [4, 10, 11, 21]. The non-free case lies beyond the scope of this work but it can also be treated using the theory of p-basis and p-generating sequences, see for instance [11, 12, 18, 21].

3.1. Convolutional codes

Definition 3.1. *A convolutional code $\mathcal{C}$ of rate k/n is a free submodule of $\mathbb{Z}_{p^r}[d]^n$ of rank k. A matrix $G(d) \in \mathbb{Z}_{p^r}[d]^{k\times n}$ whose rows form a basis of $\mathcal{C}$ is called an encoder of $\mathcal{C}$.*

Thus, an encoder of $\mathcal{C}$ is a full row rank matrix $G(d) \in \mathbb{Z}_{p^r}[d]^{k\times n}$ such that

$$\mathcal{C} \quad = \quad \text{Im}_{\mathbb{Z}_{p^r}[d]} G(d) = \{u(d)G(d) \,:\, u(d) \in \mathbb{Z}_{p^r}[d]^k\}.$$

Equivalent encoders are full row rank matrices that are encoders of the same code. Then two equivalent encoders $G_1(d), G_2(d) \in \mathbb{Z}_{p^r}[d]^{k\times n}$ are such that $G_2(d) = U(d)G_1(d)$ for some unimodular matrix $U(d) \in \mathbb{Z}_{p^r}[d]^{k\times k}$. Thus, it follows that if a convolutional code admits a left zero-prime encoder then all its encoders are also left zero-prime. We call such codes *noncatastrophic* codes and they are the ones that admit a kernel representation as stated in the following theorem.

Theorem 3.1. *Let $\mathcal{C}$ be a convolutional code of rate k/n. Then, there exists a full column rank polynomial matrix $H(d) \in \mathbb{Z}_{p^r}[d]^{n\times(n-k)}$ such that*

$$\mathcal{C} \quad = \quad \ker_{\mathbb{Z}_{p^r}[d]} H(d) = \{w(d) \in \mathbb{Z}_{p^r}[d]^n \,:\, w(d)H(d) = 0\}$$

if and only if $\mathcal{C}$ is noncatastrophic.

Proof 4. *Let us assume first that $\mathcal{C}$ is noncatastrophic and let $G(d) \in \mathbb{Z}_{p^r}[d]^{k\times n}$ be an encoder of $\mathcal{C}$. Then, $G(d)$ is ℓZP and therefore, by Theorem 2.3, there exist polynomial matrices $B(d) \in \mathbb{F}[d]^{(n-k)\times n}$, $X(d) \in \mathbb{F}[d]^{n\times k}$ and $H(d) \in \mathbb{F}[d]^{n\times(n-k)}$ such that*

$$\begin{bmatrix} G(d) \\ B(d) \end{bmatrix} \begin{bmatrix} X(d) & H(d) \end{bmatrix} = \begin{bmatrix} X(d) & H(d) \end{bmatrix} \begin{bmatrix} G(d) \\ B(d) \end{bmatrix} = I_n$$

This means that $H(d)$ is a full column rank matrix such that $G(d)H(d) = 0$, and therefore $\mathcal{C} \subset \ker_{\mathbb{Z}_{p^r}[d]} H(d)$. On the other hand, if $w(d) \in \ker_{\mathbb{Z}_{p^r}[d]} H(d)$ we have that

$$\begin{aligned} w(d) &= w(d) \begin{bmatrix} X(d) & H(d) \end{bmatrix} \begin{bmatrix} G(d) \\ B(d) \end{bmatrix} \\ &= \begin{bmatrix} w(d)X(d) & 0 \end{bmatrix} \begin{bmatrix} G(d) \\ B(d) \end{bmatrix} \\ &= u(d)G(d), \end{aligned}$$

where $u(d) = w(d)X(d) \in \mathbb{Z}_{p^r}[d]^k$, i.e. $w(d) \in \mathcal{C}$.

For the converse let us assume that $\mathcal{C}$ is not a noncatastrophic convolutional code and that $\mathcal{C} = \ker_{\mathbb{Z}_{p^r}[d]} H(d)$ for some full column rank matrix $H(d) \in \mathbb{Z}_{p^r}[d]^{n\times(n-k)}$. Let $G(d)$ be an encoder of $\mathcal{C}$. Then, since $G(d)$ is not left zero-prime,

$$[G(d)]_p = X(d)\tilde{G}(d) \mod p$$

for some invertible but nonunimodular matrix $X(d) \in \mathbb{Z}_p[d]^{k\times k}$ *and* $\tilde{G}(d) \in \mathbb{Z}_p[d]^{k\times n}$. *Considering* $X(d)$ *and* $\tilde{G}(d)$ *as matrices over* $\mathbb{Z}_{p^r}[d]$, *we have that*

$$p^{r-1}G(d) = p^{r-1}X(d)\tilde{G}(d)$$

and therefore

$$p^{r-1}X(d)^{-1}G(d) = p^{r-1}\tilde{G}(d).$$

Since $X(d)$ *is not unimodular, there exists an* $i \in \{1,\dots,k\}$ *such that the i-th row of* $p^{r-1}X(d)^{-1}$ *is not polynomial. Let us represent such row by* $\ell_i(d)$, *i.e.,* $\ell_i(d) = e_i p^{r-1}X(d)$, *where* e_i *is the i-th vector of the canonical basis. Then* $\ell_i(d)G(d)$ *does not belong to* $\mathcal{C}$ *because* $\ell_i(d)$ *is not polynomial, but since* $\ell_i(d)G(d) = e_i p^{r-1}\tilde{G}(d)$ *is a polynomial vector, it follows that* $\ell_i(d)G(d)$ *belongs to* $\ker_{\mathbb{Z}_{p^r}[d]} H(d)$, *which is a contradiction.*

If $\mathcal{C}$ is a noncatastrophic convolutional code, then a full column rank polynomial matrix $H(d)$ such that $\mathcal{C} = \ker_{\mathbb{Z}_{p^r}[d]} H(d)$ is called a *parity-check matrix* of $\mathcal{C}$.

We conclude this section by giving a result on the relation between the order of an information sequence $u(d)$ and the corresponding codeword $w(d) = u(d)G(d)$ where $G(d)$ is an encoder. This relation will be useful later on the paper.

Let $a \in \mathbb{Z}_{p^r}$. We define the order of a to be ℓ, and we write $ord(a) = \ell$, if the set $a\mathbb{Z}_{p^r}$ has p^ℓ elements. Then, $ord(a) = \ell$ if and only if $p^{\ell-1}a$ is a nonzero element of $p^{r-1}\mathbb{Z}_{p^r}$ and $p^\ell a = 0$. In the same way we define the order of a polynomial vector $w(d) \in \mathbb{Z}_{p^r}[d]^m$ to be ℓ, and we write $ord(w) = \ell$, if $p^{\ell-1}w(d) \neq 0$ and $p^\ell w(d) = 0$. This means that $p^{\ell-1}w(d)$ is a nonzero element of $p^{r-1}\mathbb{Z}_{p^r}[d]^m$. The following lemma relates the orders of an information sequence and the corresponding codeword. We omit the simple proof.

Lemma 3.1. *Let* $\mathcal{C}$ *be a convolutional code of rate* k/n, $G(d)$ *an encoder of* $\mathcal{C}$ *and* $w(d) = u(d)G(d)$, *with* $u(d) \in \mathbb{Z}_{p^r}[d]^k$, *a codeword of* $\mathcal{C}$. *Then*

$$ord(w) = ord(u).$$

3.2. Distance properties

Next we study the free distance and column distances of a convolutional code over $\mathbb{Z}_{p^r}$. Such distances were also investigated in [18, 19, 21] for not necessarily free convolutional codes using the notion of p-basis, see [19, 21]. For the free case addressed in this work we introduce the notion of b-degree of a code and derive new bounds on the free and column distance in terms of the length, dimension and b-degree of the code. First, we formally present the definitions of free distance and column distance.

The free distance of a convolutional code is defined as

$$d_{\text{free}}(\mathcal{C}) = \min\{\text{wt}(w(d)) \,:\, w(d) \in \mathcal{C},\, w(d) \neq 0\}$$

where for $w(d) = \sum_{i \in \mathbb{N}_0} w_i d^i$, $\mathrm{wt}(w(d)) = \sum_{i \in \mathbb{N}_0} \mathrm{wt}(w_i)$, with $\mathrm{wt}(w_i)$ to be the number of nonzero entries of w_i. Let $[\mathcal{C}]_p = \{[w(d)]_p : \ w(d) \in \mathcal{C}\}$ and define

$$d_{\mathrm{free}}([\mathcal{C}]_p) = min\{wt(v(d)) : \ v(d) \in [\mathcal{C}]_p, \, v(d) \neq 0\}.$$

In [21, Theorem 5.3] it was shown that

$$d_{\mathrm{free}}(\mathcal{C}) \geq d_{\mathrm{free}}([\mathcal{C}]_p). \tag{1}$$

This can be alternatively shown as follows. Note that $[\mathcal{C}]_p \simeq p^{r-1}\mathcal{C}$ and that $d_{\mathrm{free}}([\mathcal{C}]_p) = d_{\mathrm{free}}(p^{r-1}\mathcal{C})$ with $d_{\mathrm{free}}(p^{r-1}\mathcal{C}) = \min\{\mathrm{wt}(p^{r-1}w(d)) : w(d) \in \mathcal{C}, [w(d)]_p \neq 0\}$. Let $w(d)$ be a nonzero codeword of $\mathcal{C}$ of order ℓ. Lemma 3.1 implies that $p^{\ell-1}w(d)$ is a nonzero vector of $p^{r-1}\mathcal{C}$, and since

$$\mathrm{wt}(w(d)) \geq \mathrm{wt}(p^{\ell-1}w(d))$$

the inequality (1) follows. Next theorem shows that inequality (1) is in fact an equality.

Theorem 3.2. *Let $\mathcal{C}$ be a convolutional code. Then*

$$d_{\mathrm{free}}(\mathcal{C}) = d_{\mathrm{free}}([\mathcal{C}]_p).$$

Proof 5. *We only need to prove that*

$$d_{\mathrm{free}}(\mathcal{C}) \leq d_{\mathrm{free}}([\mathcal{C}]_p).$$

For that let $w(d)$ be a nonzero codeword of $[\mathcal{C}]_p$. Then there exists $\tilde{w}(d) \in \mathcal{C}$ such that $[\tilde{w}(d)]_p = w(d)$. Thus, $p^{r-1}\tilde{w}(d) \in \mathcal{C}$ with $\mathrm{wt}(p^{r-1}\tilde{w}(d)) = \mathrm{wt}(w(d))$, which implies that $d_{\mathrm{free}}(\mathcal{C}) \leq d_{\mathrm{free}}([\mathcal{C}]_p)$.

The maximum value that the free distance of a convolutional code over a finite field of rate k/n can attain depends also of the degree of the code which is defined as the maximum of the degrees of the determinants of the submatrices of one and hence any generator matrix of $\mathcal{C}$. If $\mathcal{C}$ is a convolutional code over a finite field of rate k/n and degree δ, then

$$d_{\mathrm{free}}(\mathcal{C}) \leq (n-k)\left(\lfloor \frac{\delta}{k} \rfloor + 1\right) + \delta + 1. \tag{2}$$

This upper bound is called the Generalized Singleton bound and was found first in [23] in the field case and then extended in [19, 21] for the ring case using the notion of p-degree that is not used in this work.

For the case of free modules of $\mathbb{Z}_{p^r}^n$ that is considered here we will obtain a new expression for the bound on the free distance of a free convolutional code $\mathcal{C}$. For that we need to introduce the novel concept of b-degree of $\mathcal{C}$.

Definition 3.2. *Let $\mathcal{C}$ be a convolutional code over $\mathbb{Z}_{p^r}[d]$. The b-degree of $\mathcal{C}$ is equal to the degree of $[\mathcal{C}]_p$.*

The b-degree of a convolutional code $\mathcal{C}$ can be easily obtained by calculating the maximum degree of the full size minors of $[G(d)]_p \bmod p$, for any encoder $G(d)$ of $\mathcal{C}$.

The next result follows immediately from Theorem 3.2, Definition 3.2 and from the expression (2).

Theorem 3.3. *Let $\mathcal{C}$ be a convolutional code of rate k/n and b-degree δ. Then*

$$d_{\text{free}}(\mathcal{C}) \leq (n-k)\left(\lfloor \frac{\delta}{k} \rfloor + 1\right) + \delta + 1.$$

A convolutional code of rate k/n and b-degree δ with free distance $(n-k)\left(\lfloor \frac{\delta}{k} \rfloor + 1\right) + \delta + 1$ is said to be a Maximum Distance Separable (MDS) code. It follows immediately from Theorem 3.2 that a convolutional code $\mathcal{C}$ is MDS if and only if $[\mathcal{C}]_p$ is also MDS over $\mathbb{Z}_p[d]$.

Another type of distances of a convolutional code which can be very useful in sequential decoding and have showed to have a potential use in streaming applications are the column distances [14].

Let $G(d)$ be an encoder of $\mathcal{C}$ and let us write $G(d) = \sum_{i=0}^{\nu} G_i d^i, \quad G_i \in \mathbb{Z}_{p^r}^{k\times n}$. The codeword $w(d) = \sum_{i\in\mathbb{N}_0} w_i d^i$, $w_i \in \mathbb{Z}_{p^r}^n$, corresponding to $u(d) = \sum_{i\in\mathbb{N}_0} u_i d^i$, $u_i \in \mathbb{Z}_{p^r}^k$, is such that

$$[w_0\ w_1\ \cdots\ w_j] = [u_0\ u_1\ \cdots\ u_j]G_j^c$$

where

$$G_j^c = \begin{bmatrix} G_0 & G_1 & \cdots & G_j \\ & G_0 & \ldots & G_{j-1} \\ & & \ddots & \\ & & & G_0 \end{bmatrix}$$

is called the truncated sliding matrix corresponding to $G(d)$ (we consider $G_j = 0$, if $j > \nu$), [7, 18].

Definition 3.3. *[18, 27] Given an encoder $G(d)$ of a convolutional code $\mathcal{C}$, we define the j-th column distance of $G(d)$ as*

$$d_j^c(G) = \min\{\text{wt}([u_0\ u_1\ \cdots\ u_j]G_j^c) : u_i \in \mathbb{Z}_{p^r}^k,\ u_0 \neq 0\}.$$

Parity-check matrices are very useful in the analysis of such distances. For this reason we restrict the study of such distances to noncatastrophic convolutional codes. Note that if $G(d)$ is an encoder of a noncatastrophic convolutional code $\mathcal{C}$, then $G(d)$ has a right polynomial inverse and therefore $G(0)$ is full row rank and this means that the j-th column distance of $\mathcal{C}$ is an invariant of the code and can be obtained as

$$d_j^c(\mathcal{C}) = \min\{\text{wt}([w_0\ w_1\ \cdots\ w_j]) :\ [w_0\ w_1\ \cdots\ w_j] \in\ \text{Im}\ G_j^c,\ w_0 \neq 0\}.$$

If $H(d) = \sum_{i=0}^{\ell} H_i d^i,\ H_i \in \mathbb{Z}_{p^r}^{(n-k)\times n}$ is a parity-check of $\mathcal{C}$ and $H(\ell) \neq 0$, $\ell \in \mathbb{N}$, then

$$d_j^c(\mathcal{C}) = \min\{\mathrm{wt}([w_0\ w_1\ \cdots\ w_j]) :\ [w_0\ w_1\ \cdots\ w_j](H_j^c) = 0,\ w_0 \neq 0\},$$

where

$$H_j^c = \begin{bmatrix} H_0 & H_1 & \cdots & H_j \\ & H_0 & \cdots & H_{j-1} \\ & & \ddots & \vdots \\ & & & H_0 \end{bmatrix},$$

with $H_j = 0$ for $j > \ell$. The following theorem is immediate and its proof is analogous to the field case.

Theorem 3.4. *Let $\mathcal{C}$ be a noncatastrophic convolutional code of rate k/n. Then, for any $j, d \in \mathbb{N}$, $d_j^c(\mathcal{C}) = d$ if and only if the following conditions are satisfied:*

1. *there exist d rows of H_j^c linearly dependent over $\mathbb{Z}_{p^r}[d]$ such that one of these rows belongs to the first n rows of H_j^c;*
2. *all $d-1$ rows, in which one of the rows belongs to the first n rows of H_j^c, are linearly independent over $\mathbb{Z}_{p^r}[d]$.*

Remark 3.1. *Since the lines of a matrix A are linearly independent if and only if $[A]_p$ is a full row rank, the conditions 1 and 2 of the Theorem 3.4 can be expressed, respectively, and in an equivalent way, as follows:*

1. *there exist d rows of $[H_j^c]_p$ linearly dependent over $\mathbb{Z}_p[d]$ such that one of these rows belongs to the first n rows of $[H_j^c]_p$;*
2. *all $d-1$ rows, in which one of the rows belongs to the first n rows of $[H_j^c]_p$, are linearly independent over $\mathbb{Z}_p[d]$.*

Next theorem provides upper bounds on the column distances of a noncatastrophic convolutional code. These upper bounds were found in [18] for the more general case in which the convolutional codes are not necessarily noncatastrophic free convolutional codes. Although the result is not new, we opted to present the proof, because it is much simpler than the one in [18].

Theorem 3.5. *Let $\mathcal{C}$ be a noncatastrophic convolutional code of rate k/n. Then*

$$d_j^c(\mathcal{C}) \leq (n-k)(j+1)+1,$$

for all $j \in \mathbb{N}_0$.

Proof 6. *Since $\mathcal{C}$ is a noncatastrophic convolutional code over $\mathbb{Z}_{p^r}$, then$[\mathcal{C}]_p$ is a noncatastrophic convolutional code code over $\mathbb{Z}_p$ of rate k/n, and therefore*

$$d_j^c([\mathcal{C}]_p) \leq (n-k)(j+1)+1,$$

for all $j \in \mathbb{N}_0$ (see [7]). Let $w(d) = \sum_{i\in\mathbb{N}_0} w_i d^i \in [\mathcal{C}]_p$ with $w_0 \neq 0$, then

$$\mathrm{wt}([w_0\ w_1\ \cdots\ w_j]) \leq (n-k)(j+1)+1.$$

Let us consider $[w_0\ w_1\ \cdots\ w_j]$ *as a vector of* $\mathbb{Z}_{p^r}^{n(j+1)}$. *Then,* $\tilde{w}(d) = p^{r-1}w(d) \in p^{r-1}\mathcal{C}$ *is such that* $\tilde{w}(0) \neq 0$ *and* $\mathrm{wt}([\tilde{w}_0\ \tilde{w}_1\ \cdots\ \tilde{w}_j]) = \mathrm{wt}([w_0\ w_1\ \cdots\ w_j])$. *Then* $d_j^c(\mathcal{C}) \leq (n-k)(j+1)+1$.

The next result readily follows from [7, Theorem 2.4] and Remark 3.1.

Theorem 3.6. *Let* $G(d)$ *be an encoder of a noncatastrophic convolutional code over* $\mathbb{Z}_{p^r}[d]$, $\mathcal{C}$, *of rate* k/n, $k \leq n$, *and* $H(d)$ *be a parity-check matrix of* $\mathcal{C}$. *The following are equivalent:*

1. $d_j^c(\mathcal{C}) = (n-k)(j+1)+1$.
2. *every* $(j+1)k \times (j+1)k$ *full-size minor of* $[G_j^c]_p$ *formed from the columns with indices* $1 \leq t_1 < \ldots < t_{(j+1)k}$, *where* $t_{sk+1} > sn$, $s = 1, \ldots, j$,*is nonzero.*
3. *every* $(j+1)(n-k) \times (j+1)(n-k)$ *full-size minor of* $[H_j^c]_p$ *formed from the columns with indices* $1 \leq r_1 < \ldots < r_{(j+1)(n-k)}$, *where* $r_{s(n-k)} \leq sn$, $s = 1, \ldots, j$, *is nonzero.*

The column distances of a noncatastrophic $\mathcal{C}$ do not grow indefinitely, since they are naturally upper bounded by the free distance of $\mathcal{C}$. If $\mathcal{C}$ is a noncatastrophic convolutional code over a finite field of rate k/n and degree δ, then $\mathcal{C}$ can have maximum column distances up to the *L-th* column distance, where $L = \left\lfloor \frac{\delta}{k} \right\rfloor + \left\lfloor \frac{\delta}{n-k} \right\rfloor$. L is the largest integer for which

$$(n-k)(L+1)+1 \leq (n-k)\left(\left\lfloor \frac{\delta}{k} \right\rfloor + 1\right) + \delta + 1.$$

Definition 3.4. *[7] Let* $\mathcal{C}$ *be a noncatastrophic code over a finite field* $\mathbb{F}$, *of rate* k/n *and degree* δ. *Let* $L = \left\lfloor \frac{\delta}{k} \right\rfloor + \left\lfloor \frac{\delta}{n-k} \right\rfloor$. $\mathcal{C}$ *is a Maximum Distance Profile (MDP) convolutional code if*

$$d_j^c(\mathcal{C}) = (n-k)(j+1)+1, \quad \textit{for all } j \leq L.$$

Since the upper bounds of the column distances and the generalized Singleton bound coincide with the counterpart notions of $[\mathcal{C}]_p$, if $\mathcal{C}$ is a noncatastrophic convolutional code over $\mathbb{Z}_{p^r}[d]$ of rate k/n and b-degree δ then $\mathcal{C}$ also can achieve the upper bound for column distance only up to the instant *L-th*. This leads to the following definition.

Definition 3.5. *Let* $\mathcal{C}$ *be a noncatastrophic code over* $\mathbb{Z}_{p^r}[d]$, *of rate* k/n *and* b*-degree* δ. *Let* $L = \left\lfloor \frac{\delta}{k} \right\rfloor + \left\lfloor \frac{\delta}{n-k} \right\rfloor$. $\mathcal{C}$ *is a Maximum Distance Profile (MDP) convolutional code if*

$$d_j^c(\mathcal{C}) = (n-k)(j+1)+1, \quad \textit{for all } j \leq L.$$

Theorem 3.7. *Let $\mathcal{C}$ be a noncatastrophic code over $\mathbb{Z}_{p^r}[d]$, of rate k/n and b-degree δ. $\mathcal{C}$ is an MDP code if and only if $[\mathcal{C}]_p$ is an MDP code over $\mathbb{Z}_p[d]$.*

Proof 7. *Let $\mathcal{C}$ be an MDP convolutional code, $j \leq L = \left\lfloor \frac{\delta}{k} \right\rfloor + \left\lfloor \frac{\delta}{n-k} \right\rfloor$ and $\tilde{w}(d) = \sum_{i \in \mathbb{N}_0} \tilde{w}_i d^i \in [\mathcal{C}]_p,\ \tilde{w}_0 \neq 0$*

Let us consider $w(d)$ as a vector of $\mathbb{Z}_{p^r}[n]^n$, and let $w(d) = \sum_{i \in \mathbb{N}_0} w_i d^i; p^{r-1}\tilde{w}(d) \in \mathcal{C},\ w_0 = p^{r-1}\tilde{w}_0 \neq 0$. Since $wt([\ \tilde{w}_0\ \tilde{w}_1\ \ldots\ \tilde{w}_j\ ]) = wt([\ w_0\ w_i\ \ldots\ w_j\ ])$ and $\mathcal{C}$ is an MDP convolutional code and $d_j^c(\mathcal{C}) \leq wt([\ w_0\ w_i\ \ldots\ w_j\ ])$, it follows that

$$(n-k)(j+1)+1 \leq wt([\ \tilde{w}_0\ \tilde{w}_1\ \ldots\ \tilde{w}_j\ ]),\ j \leq L$$

and therefore $[\mathcal{C}]_p$ is a MDP code.

Let us now consider $[\mathcal{C}]_p$ a MDP code and $w(d) = \sum_{i \in \mathbb{N}_0} w_i d^i \in \mathcal{C},\ w_0 \neq 0,\ j \leq L = \left\lfloor \frac{\delta}{k} \right\rfloor + \left\lfloor \frac{\delta}{n-k} \right\rfloor$, ℓ the order of $[\ w_0\ w_1\ \ldots\ w_j\ ]$ and s_1 the smallest integer less than or equal to j, such that w_{s_1} has order ℓ_1. It follows that $p^{r-l}[\ w_0\ w_1\ \ldots\ w_j\ ] = p^{r-1}[\ 0\ 0\ \tilde{w}_{s_1}\ \ldots\ \tilde{w}_j\ ]$, with $[\tilde{w}_{s_1}]_p \neq 0$. Let $p^{r-l}w(d) = d^s(p^{r-1}\tilde{w}(d))$, $\tilde{w}(d) = \sum_{i \in \mathbb{N}_0} \tilde{w}_{s_1+i}\, d^i$, be a codeword. Since $G(d)$ is a left-zero prime matrix, $G(0)$ is full row rank. So $d^s(p^{r-1}\tilde{w}(d)) = (d^s u(d))G(d)$ and, therefore, $p^{r-1}\tilde{w}(d) = u(d)G(d)$, which implies that $p^{r-1}\tilde{w}(d) \in \mathcal{C}$. That way, $[\tilde{w}(d)]_p \in [\mathcal{C}]_p$ and

$$wt\left([\ p^{r-1}\tilde{w}_{s_1}\ \ldots\ p^{r-1}\tilde{w}_{j-s_1}\ ]\right) \quad = \quad wt\left([\ \tilde{w}_{s_1}\ \ldots\ \tilde{w}_{j-s_1}\ ]_p\right), \quad [\tilde{w}_{s_1}]_p \neq 0.$$

Furthermore, $[\mathcal{C}]_p$ is MDP, so

$$wt\left([\ p^{r-1}\tilde{w}_{s_1}\ \ldots\ p^{r-1}\tilde{w}_{j-s_1}+1\ ]\right) \geq (n-k)(j-s_1+1)+1.$$

Let us now consider $[\ w_0\ w_1\ \ldots\ w_{s_1-1}\ ]$ with order $\ell_2 \leq \ell$, such that

$$p^{r-l_2}[\ w_0\ w_1\ \ldots\ w_{s_1-1}\ ] = p^{r-1}[\ 0\ 0\ \tilde{\tilde{w}}_{s_2}\ \ldots\ \tilde{\tilde{w}}_{s_1-1}\ ],$$

with $s_2 \leq s_1 - 1$ and $[\tilde{\tilde{w}}_{s_2}(d)]_p \neq 0$. Repeating the previous reasoning, we have to

$$wt\left([\ p^{r-1}\tilde{w}_{s_2}\ \ldots\ p^{r-1}\tilde{w}_{s_1-1}\ ]\right) \geq (n-k)(s_1-1+s_2+1)+1 = (n-k)(s_1+s_2)+1$$

Successively applying the previous process, we obtain

$$wt\left([\ w_0\ w_1\ \ldots\ w_j\ ]\right) \geq (n-k)(j+1)+1.$$

According to this theorem, we can easily get an MDP code over $\mathbb{Z}_{p^r}[d]$ of rate k/n and b-degree δ, from an MDP code over $\mathbb{Z}_p[d]$, of rate k/n and degree δ.

4. Conclusions and future work

In this paper we have investigated the central notion of primeness of polynomial matrices over $\mathbb{Z}_{p^r}$. We showed that zero left prime encoders define noncatastrophic convolutional codes over $\mathbb{Z}_{p^r}$ and allow a representation of the convolutional code by means of a polynomial parity-check matrix. We have studied free and columns distances of these codes and show that these are determined by the projection of the code over $\mathbb{Z}_p$. A natural and interesting avenue for future investigation is to generalized these results to wider classes of rings such as finite chain rings [2].

5. Acknowledgments

The second and third authors were supported by The Center for Research and Development in Mathematics and Applications (CIDMA) through the Portuguese Foundation for Science and Technology (FCT - Fundação para a Ciência e a Tecnologia), references UIDB/04106/2020 and UIDP/04106/2020. Diego Napp is partially supported by Ministerio de Ciencia e Innovación via the grant with ref. PID2019-108668GB-I00.

References

[1] G. N. Alfarano and J. Lieb. On the left primeness of some polynomial matrices with applications to convolutional codes. *Journal of Algebra and Its Applications*, https://doi.org/10.1142/S0219498821502078, 2020.

[2] R. Lamia Bouzara, K. Guenda, and E. MartÃnez-Moro. Lifted codes and lattices from codes over finite chain rings, 2020.

[3] A. R. Calderbank and N. J. A. Sloane. Modular and p-adic cyclic codes. *Designs, Codes and Cryptography*, 6(1):21–35, 1995.

[4] N. DeCastro-GarcÃa. Feedback equivalence of convolutional codes over finite rings. *Open Mathematics*, 15(1):1495 – 1508, 2017.

[5] E. Fornasini and R. Pinto. Matrix fraction descriptions in convolutional coding. *Linear Algebra and its Applications*, 392:119 – 158, 2004.

[6] G.D. Forney. Convolutional Codes I: Algebraic Structure. *IEEE Trans. Inform. Theory*, 16:720–738, 1970. Correction, Ibid., IT-17,pp. 360, 1971.

[7] H. Gluesing-Luerssen, J. Rosenthal, and R. Smarandache. Strongly MDS convolutional codes. *IEEE Trans. Inform. Theory*, 52(2):584–598, 2006.

[8] R. Johannesson, Z.X. Wan, and E. Wittenmark. Some structural properties of convolutional codes over rings. *IEEE Trans. Inform. Theory*, 44(2):839–845, 1998.

[9] R. Johannesson and K. Sh. Zigangirov. *Fundamentals of Convolutional Coding*. IEEE Press, New York, 2015.

[10] M. Kuijper and R. Pinto. Minimal trellis construction for finite support convolutional ring codes. *Lecture Notes in Computer Science*, 5228:95–106, 2008.

[11] M. Kuijper and R. Pinto. On minimality of convolutional ring encoders. *IEEE Trans. Automat. Contr.*, 55)(11):4890 –4897, 2009.

[12] M. Kuijper and R. Pinto. An iterative algorithm for parametrization of shortest length linear shift registers over finite chain rings. *Designs, Codes and Cryptography*, 83(2):283–305, May 2017.

[13] M. Kuijper, R. Pinto, and J. W. Polderman. The predictable degree property and row reducedness for systems over a finite ring. *Linear Algebra and its Applications*, 425(2–3):776–796, 2007.

[14] J. Lieb. Complete MDP convolutional codes. *Journal of Algebra and Its Applications*, 18(06):1950105, 2019.

[15] Z. Lin and N.K. Bose. A generalization of serre's conjecture and some related issues. *Linear Algebra and its Applications*, 338(1):125 – 138, 2001.

[16] J. Liu, T. Wu, D. Li, and J. Guan. On zero left prime factorizations for matrices over unique factorization domains. *Mathematical Problems in Engineering*, (https://doi.org/10.1155/2020/1684893), 2020.

[17] J. L. Massey and T. Mittelholzer. Convolutional codes over rings. *In Proc. 4th Joint Swedish-Soviet Int. Workshop Information Theory*, pages 14–18, 1989.

[18] D. Napp, R. Pinto, and M. Toste. Column distances of convolutional codes over $\mathbb{Z}_{p^r}$. *IEEE Trans. Inform. Theory*, 65(2):1063–1071, 2017.

[19] D. Napp, R. Pinto, and M. Toste. On MDS convolutional codes over $\mathbb{Z}_{p^r}$. *Designs, Codes and Cryptography*, 83:101–114, 2017.

[20] D. Napp and P. Rocha. Autonomous multidimensional systems and their implementation by behavioral control. *Systems & Control Letters*, 59(3–4):203–208, 2010.

[21] M. El Oued and P. Solé. MDS convolutional codes over a finite ring. *IEEE Trans. Inform. Theory*, 59(11):7305 – 7313, 2013.

[22] J. Rosenthal. An optimal control theory for systems defined over finite rings. In V.D. Blondel, E.D. Sontag, M. Vidyasagar, and J.C. Willems, editors, *Open Problems in Mathematical Systems and Control Theory*, pages 192–201. Springer-Verlag, 1998.

[23] J. Rosenthal. An algebraic decoding algorithm for convolutional codes. In G. Picci and D.S. Gilliam, editors, *Dynamical Systems, Control, Coding, Computer Vision: New Trends, Interfaces, and Interplay*, pages 343–360. Birkäuser, Boston-Basel-Berlin, 1999.

[24] S. Shankar. The hautus test and genericity results for controllable and uncontrollable behaviors. *SIAM J. Control Optim.*, 52:32–51, 2014.

[25] P. Sole and V. Sison. Quaternary convolutional codes from linear block codes over galois rings. *IEEE Trans. Information Theory*, 53:2267–2270, 2007.

[26] D. Sridhara and T.E. Fuja. LDPC codes over rings for PSK modulation. *IEEE Trans. Inf. Th.*, 51(9):3209–3220, 2005.

[27] M. Toste. *Distance properties of convolutional codes over* $\mathbb{Z}_{p^r}$. University of Aveiro, September 2016. PhD Thesis.

[28] E. Zerz. Primeness of multivariate polynomial matrices. *Systems Control Lett.*, 29(3):139–145, 1996.